2-16-00

A

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1 53(b))

Attorney Docket No.	190-1445
First Inventor or Application Identifier	Bunn
Title	Printed Document Authentication
Express Mail Label No.	EL 388 801 925 US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] * **Fee Transmittal Form** *(e.g., PTO/SB/17)*
   (Submit an original and a duplicate for fee processing)

2. [X] **Specification** [Total Pages 11]
   (preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure

3. [X] **Drawing(s)** *(35 U.S.C. 113)* [Total Sheets 3]

4. **Oath or Declaration** [Total Pages 3]
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d))
      (for continuation/divisional with Box 16 completed)
      i. [ ] DELETION OF INVENTOR(S)
         Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. [ ] Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission
   (if applicable, all necessary)
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [X] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement [ ] Power of Attorney *(when there is an assignee)*
9. [ ] English Translation Document *(if applicable)*
10. [X] Information Disclosure Statement (IDS)/PTO-1449 [X] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. [ ] * Small Entity Statement(s) (PTO/SB/09-12) [ ] Statement filed in prior application, Status still proper and desired
14. [X] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. [ ] Other: ....

16. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No· _____/_____

Prior application information: Examiner _____ Group / Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label
(Insert Customer No or Attach bar code label here)
or [X] Correspondence address below

Name	William M. Lee, Jr.
	Lee, Mann, Smith, McWilliams, Sweeney & Ohlson
Address	P.O. Box 2786
City	Chicago
State	Illinois
Zip Code	60690-2786
Country	USA
Telephone	(312) 368-1300
Fax	(312) 368-0034

Name (Print/Type)	William M. Lee, Jr	Registration No. (Attorney/Agent)	26,935
Signature		Date	2/15/00

Burden Hour Statement· This form is estimated to take 0 2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

PRINTED DOCUMENT AUTHENTICATION

Background to the Invention

This invention relates to a method and apparatus for authenticating printed documents.

It is frequently required to provide some way of checking the authenticity of printed documents, to confirm that the document has been issued from a particular source, and that the information in it has not been tampered with. In particular, such authentication may be required for certificates of various kinds.

As an example, in the UK it is a requirement that any road vehicle over three years old should have a test certificate, referred to as an MOT certificate. These certificates are issued by licensed vehicle testing stations, following an inspection of the vehicle to check its roadworthiness and compliance with legal requirements. The certificate must be presented at a post office when the owner of the vehicle re-licenses it. Clearly, the post office should check that the certificate is not a forgery, and that the information in it has not been altered. At present, the post office clerk does this simply by making a visual check.

The object of the invention is to provide an improved method for authenticating printed documents.

Summary of the Invention

According to the invention a method for authenticating a printed document comprises the following steps:
a) a document producer sends information to be included in a
   document to an authentication authority;

b) the authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer;

c) the document producer prints the document, including both the information and the authentication code; and

d) a document checker cryptographically checks the authentication code against the information in the document.

In the MOT certificate example described above, the document producer would be the vehicle testing station, the authentication authority may be a central agency run by (or with powers delegated by) the government Vehicle Inspectorate (VI), and the document checker may be the post office at which the MOT is presented.

The authentication code may be generated and checked using a cryptographic key associated with the authentication authority. A secret key, known to both the authentication authority and the document checker, may be used. Alternatively, a public/private key pair may be used where the authentication code is generated using the authentication authority's private key and checked using its public key.

One document authentication method in accordance with the invention will now be described by way of example with reference to the accompanying drawings.

Brief Description of the Drawings

Figure 1 is a schematic diagram of a system for issuing and authenticating certificates.

Figure 2 is a flow chart showing the operation of a software component for issuing certificates.

Figure 3 is a schematic diagram showing a certificate produced
by the system.

Description of an Embodiment of the Invention

Referring to Figure 1, the system involves the following
entities:

* VI Data Centre 101. This is a central agency, run by the
  Vehicle Inspectorate (VI).
* Vehicle testing stations (VTS) 102. These are authorised by
  the VI to test vehicles and to issue MOT certificates. Each
  vehicle testing station may employ one or more authorised
  vehicle testers to carry out the tests.
* Post Offices 103.

The VI Data Centre includes a central server computer 104, and a
database 105. The database holds details of all licensed
vehicles, vehicle testing stations, and authorised vehicle
testers. The VI Data Centre has a secret key, referred to
herein as the VI secret key, which in this example is known to
both the VI data centre and the post offices.

Each of the vehicle testing stations 102 has a computer terminal
106, which can communicate with the central server 104 by way of
a network 107. The terminal is connected to a printer 108,
which is used for printing the MOT test certificates 109. The
printer 108 incorporates a barcode scanner, so that it can read
barcodes on blank certificates inserted into the printer.

Each of the terminals 106 includes communications software,
which manages communications between terminal and the central
server. All communications between terminal and the central
server are encrypted, to ensure that messages cannot be
intercepted. In addition, security technology is used to verify

the authenticity of both ends of the link, to prevent a rogue
device from linking into the network and pretending to be a
terminal.

In operation, a vehicle tester can enter information relating to
a particular vehicle test into the terminal. The terminal
includes a function which allows the vehicle tester to confirm
the results of a test and, if the results are confirmed, to
print a test certificate or failure notice as appropriate.
Figure 2 shows this function in more detail.

(Step 201) The function first displays the test information,
with the overall result (pass or fail) summarised.

(Step 202) The function then asks the tester to confirm whether
or not the test results are correct. If they are not correct,
the function exits, and the tester may then go back to change
the test information.

(Step 203) If the tester confirms that the results are correct,
the function then branches according to the test result.

(Step 204) If the test result was "pass", the function prompts
the user to specify whether the test certificate is to be
printed locally, at the test station, or mailed directly from
the VI Data Centre to the registered keeper of the vehicle.

(Step 205) If the test certificate is to be printed locally, the
function prompts the user to feed a blank pass certificate into
the printer 108. Each blank pass certificate has a unique pre-
printed serial number, and a barcode containing the serial
number, as well as other security features such as a watermark.
The VI keeps a record of the serial numbers of the certificates
issued to each testing station, so that each certificate can be
traced back to a particular testing station.

(Steps 206-207) When the certificate is in the printer, the function instructs the barcode scanner incorporated in the printer to scan in the certificate serial number. The terminal then transmits a message to the central server. The message contains details of the tester and the test station, the certificate serial number, the vehicle details, and the test results.

When the central server 104 receives this message, it performs a final check to confirm that the tester and the vehicle test station are duly authorised to perform the test.

Assuming this check is satisfactory, the central server proceeds as follows. First, it generates a message authentication code (MAC) from a predetermined sub-set of information in the message. In this example, the MAC is generated by performing a key-dependent one-way hash of the information, using the VI secret key. The central server transmits this MAC back to the terminal.

(Step 208) When the terminal receives the MAC, it prints the certificate. The contents of the certificate are described below.

(Step 209) If on the other hand the test certificate is to be mailed directly to the registered keeper of the vehicle, the function transmits the test information to the central server, with a request for a mailed certificate. The central server performs checks as described above, and if these checks are satisfactory, prints the certificate.

(Steps 210 - 212) If the test result was "failure", the function prompts the user to feed a blank failure notice into the printer. The function then transmits the test information to the central server, and prints the failure notice.

Figure 3 shows the format of the certificate. It includes the following:

- Pre-printed certificate serial number 301, and pre-printed barcode (not shown) containing this serial number.
- Test date 302
- Expiry date of certificate 303.
- Vehicle details 304.
- MAC 305, as a string of characters.
- Bar code 306, representing the MAC in bar code form.

Referring again to Figure 1, each of the Post Offices 103 is provided with at least one terminal 112, having a bar code reader 113. It is assumed that the terminal has knowledge of the VI secret key.

When a vehicle owner presents an MOT certificate at the post office, the post office clerk uses the bar code reader 113 to scan the bar code 306 on the certificate, so as read the MAC into the terminal.

The clerk also types in the predetermined sub-set of information from the certificate (i.e. the same sub-set as used by the central server to generate the MAC). The terminal then uses this information, along with the VI secret key, to generate a MAC, and compares this with the MAC read from the bar code. If they are not equal, the terminal generates a message to alert the clerk.

If for any reason the bar code reader will not read the bar code, the clerk may type the MAC into the terminal, from the printed version of the VI signature.

In summary, it can be seen that the system described above allows a certificate to be authenticated quickly and easily.

Some possible modifications

It will be appreciated that many modifications may be made to the system described above without departing from the scope of the present invention. For example, instead of using a secret key to form the MAC and to check it, a public/private key pair may be used. In this case, the authentication code is generated using the authentication authority's private key and checked using its public key.

Instead of requiring the clerk to type information from the certificate into the terminal, the information could be scanned in.

Instead of requiring the clerk to scan or key in the MAC from the certificate, the terminal may display the MAC it has generated, so that the clerk can visually compare this with the MAC printed on the certificate.

The vehicle test station could be arranged to authenticate the previous year's certificate, before generating a new one.

It should be noted that the invention is not restricted to issuing of MOT certificates as described above, but can be used in any application where it is required to authenticate a printed document.

CLAIMS

1.   A method for authenticating a printed document comprising the following steps:
a) a document producer sends information to be included in a document to an authentication authority;
b) the authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer;
c) the document producer prints the document, including both the information and the authentication code; and
d) a document checker cryptographically checks the authentication code against the information in the document.

2. A method according to Claim 1 wherein the document producer includes a bar code in the document, said bar code containing the authentication code, and wherein the document authenticator is provided with means for reading the bar code to obtain the authentication code.

3. A method according to Claim 1 wherein the document includes a pre-printed serial number, which is sent to said authentication authority, and wherein said authentication authority uses said pre-printed serial number in generating said authentication code.

4. A method according to Claim 3 wherein said pre-printed serial number is included in said document as a pre-printed bar code.

5. A method according to Claim 4 wherein the document producer uses a combined printer and bar-code scanner to read said pre-printed bar code and then to print said document.

6. A method according to Claim 1 wherein said document checker performs the following steps:

a) entering said authentication code into a computer;

b) entering information in the document into the computer;

c) causing the computer to cryptographically generate a check code from said information; and

d) causing the computer to compare said check code with said authentication code and to generate a warning indication if said check code does not correspond with said authentication code.

7. A method according to Claim 1 wherein said authentication authority cryptographically generates said authentication code using a cryptographic key associated with said authentication authority.

8. A method according to Claim 7 wherein said cryptographic key is a secret key known to both the authentication authority.

9. A method according to Claim 8 wherein said authentication code is generated by performing a key-dependent one-way hash of said information, using said secret key.

10. A method according to Claim 7 wherein said authentication authority generates said authentication code using the private key of a public/private key pair, and wherein the document checker checks the authentication code using the public key of said public/private key pair.

11. A method according to Claim 1 wherein communication between said document producer and said authentication authority is protected by encryption.

12. A method according to Claim 1 wherein the document producer can specify an option of having the certificate printed by said authentication authority instead of printing the certificate locally.

13. Apparatus for authenticating a printed document, comprising:

a) a plurality of document producer stations;

b) at least one authentication service; and

c) a plurality of document checker stations;

d) wherein each document producer station includes means for inputting information to be included in a document, and means for sending said information to said authentication service;

e) wherein the authentication service includes means for cryptographically generating an authentication code from this information, and means for sending the authentication code back to the document producer staion;

f) wherein each document producer station includes means for printing the document, including both the information and the authentication code;

g) and wherein each document checker station includes means for cryptographically checking the authentication code against the information in the document.
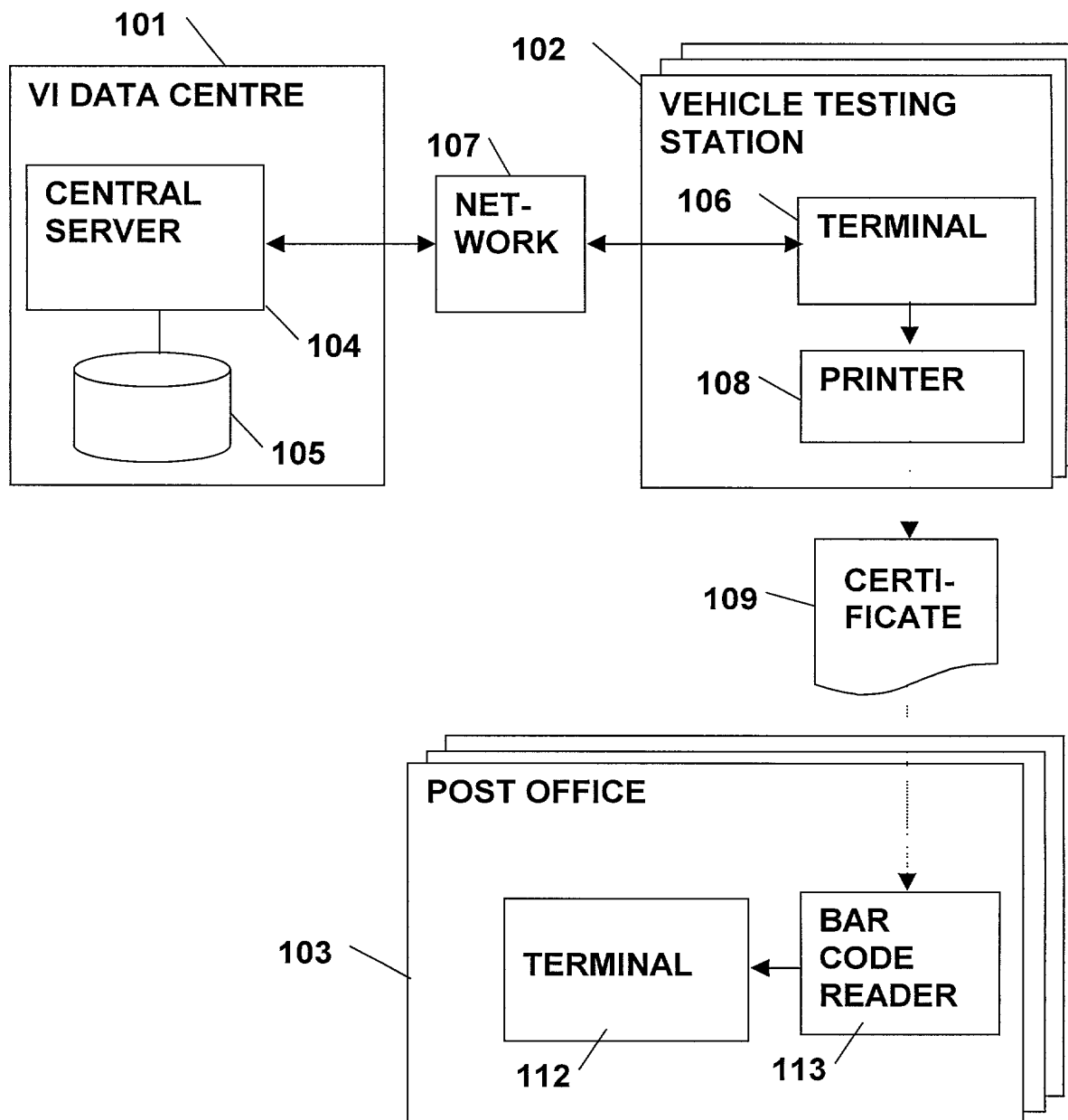

14. Apparatus according to Claim 13 wherein each of said document producer stations includes a combined printer and bar code scanner for reading from said document a pre-printed bar code containing a serial number.

15. Apparatus according to Claim 13 wherein each of said document producer stations includes means for printing bar codes on documents, and wherein each of said document checker stations includes a bar code reader for reading bar codes from documents.
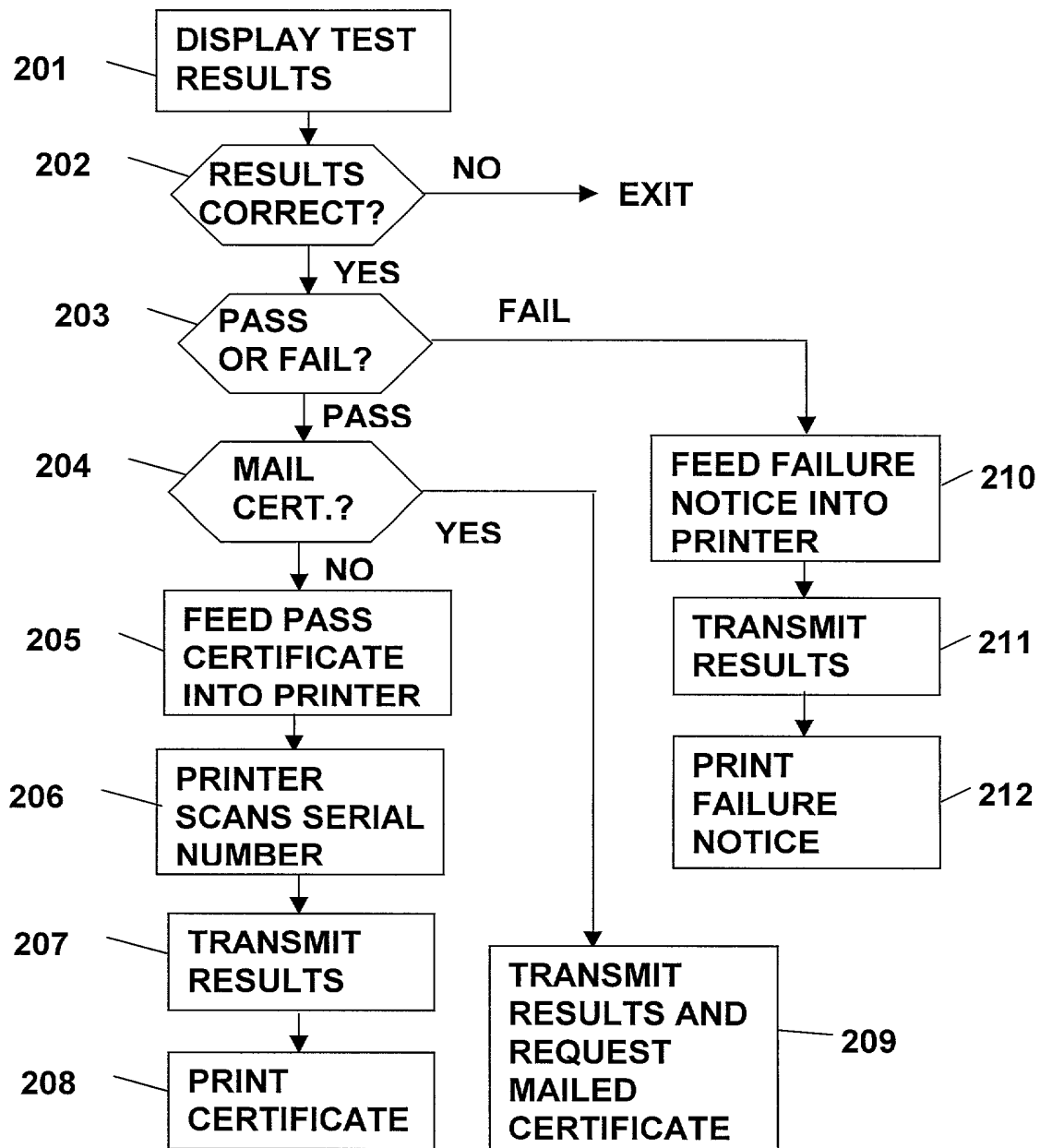
ABSTRACT

A method for authenticating a printed document is described. A document producer sends information to be included in a document to an authentication authority. The authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer. The document producer then prints the document, including both the information and the authentication code, and a bar code representing the authentication code. A document checker scans in the bar code, and cryptographically checks the authentication code against the information in the document.

FIG.1

```
          ┌─────────────────┐
   201 ─── │ DISPLAY TEST    │
          │ RESULTS         │
          └─────────────────┘
                  │
                  ▼
              ╱─────────╲        NO
   202 ──── ╱  RESULTS   ╲ ──────────────────►  EXIT
          ╲  CORRECT?   ╱
            ╲─────────╱
                │ YES
                ▼
              ╱─────────╲          FAIL
   203 ──── ╱   PASS     ╲ ──────────────────────┐
          ╲  OR FAIL?   ╱                         │
            ╲─────────╱                           │
                │ PASS                            │
                ▼                                 ▼
              ╱─────────╲                 ┌─────────────────┐
   204 ──── ╱   MAIL     ╲                │ FEED FAILURE    │ ─── 210
          ╲  CERT.?     ╱                 │ NOTICE INTO     │
            ╲─────────╱ ──────┐          │ PRINTER         │
                │ NO    YES    │          └─────────────────┘
                ▼              │                  │
          ┌─────────────────┐ │                  ▼
   205 ── │ FEED PASS       │ │          ┌─────────────────┐
          │ CERTIFICATE     │ │          │ TRANSMIT        │ ─── 211
          │ INTO PRINTER    │ │          │ RESULTS         │
          └─────────────────┘ │          └─────────────────┘
                │             │                  │
                ▼             │                  ▼
          ┌─────────────────┐ │          ┌─────────────────┐
   206 ── │ PRINTER         │ │          │ PRINT           │ ─── 212
          │ SCANS SERIAL    │ │          │ FAILURE         │
          │ NUMBER          │ │          │ NOTICE          │
          └─────────────────┘ │          └─────────────────┘
                │             │
                ▼             ▼
          ┌─────────────────┐ ┌─────────────────┐
   207 ── │ TRANSMIT        │ │ TRANSMIT        │
          │ RESULTS         │ │ RESULTS AND     │
          └─────────────────┘ │ REQUEST         │ ─── 209
                │             │ MAILED          │
                ▼             │ CERTIFICATE     │
          ┌─────────────────┐ └─────────────────┘
   208 ── │ PRINT           │
          │ CERTIFICATE     │
          └─────────────────┘
```
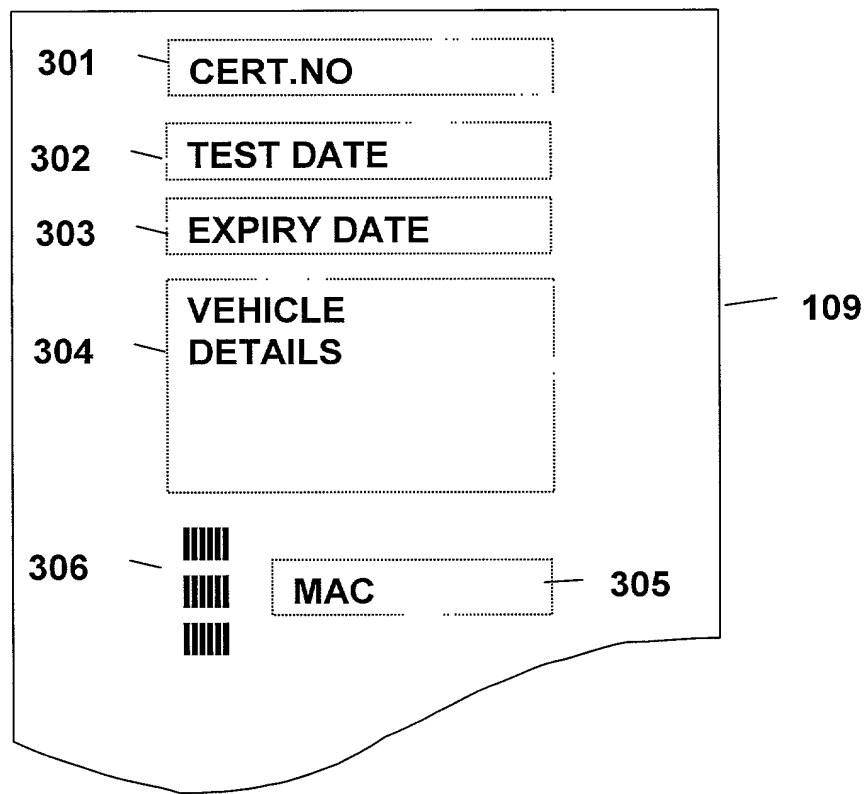
FIG.2

FIG. 3

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **Printed Document Authentication**, the specification of which:

     __X__   is attached hereto.

     _____   was filed on _____ as
              Application Serial No.
              and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

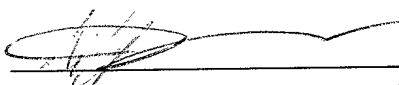|			Priority Claimed	
Country	**Number**	**Date Filed**	**Yes**	**No**
United Kingdom	9906924.7	March 26, 1999	X	___
			___	___

I hereby claim the benefit under Title 35, United States Code
Section 120 of any United States application(s) listed below and,
insofar as the subject matter of each of the claims of this
application is not disclosed in the prior United States
application in the manner provided by the first paragraph of Title
35, United States Code, Section 112, I acknowledge the duty to
disclose material information as defined in Title 37, Code of
Federal Regulations, Section 1.56(a) which occurred between the
filing date of the prior application and the national or PCT
international filing date of this application.

Application Serial No.	**Filing Date**	**Status**

And I hereby appoint Wm. Marshall Lee, Registration No. 16,853,
John M. Mann, Registration No. 17,775, Thomas E. Smith,
Registration No. 18,243, Dennis M. McWilliams, Registration No.
25,195, James R. Sweeney, Registration No. 18,721, William M. Lee,
Jr., Registration No. 26,935, Glenn W. Ohlson, Registration No.
28,455, David C. Brezina, Registration No. 34,128, Jeffrey R.
Gray, Registration No. 33,391, Timothy J. Engling, Registration
No. 39,970, Gregory B. Beggs, Registration No. 19,286, Gerald S.
Geren, Registration No. 24,528 and Peter J. Shakula, Registration
No. 40,808 as my attorneys to prosecute this application and to
transact all business in the Patent and Trademark Office connected
herewith. It is requested that all communications be directed to
Lee, Mann, Smith, McWilliams, Sweeney & Ohlson, P.O. Box 2786,
Chicago, Illinois 60690-2786, telephone number (312) 368-1300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: **Michael George Bunn**

Signature _____ Date JANUARY 27, 2000

Country of Residence: United Kingdom

Country of Citizenship: United Kingdom

Post Office and Residence Address: 197 Hyde End Road, Spencers Wood, Reading, Berkshire, RG7 1BU, England